A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

NO. 2002-0037-4T

INDEPENDENT STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT
THE GEORGE E. FINGOLD LIBRARY

July 1, 2000 Through December 17, 2001

OFFICIAL AUDIT REPORT
JANUARY 31, 2002

TABLE OF CONTENTS

INTRODUCTION

The State Library of Massachusetts was established in 1826 under Chapter 123 of the Massachusetts General Laws, (MGL). In 1960, under Chapter 380, Section 1, the name was changed to the George E. Fingold Library. The Board of Trustees of the Library, per Section 33, consists of the President of the Senate, the Speaker of the House of Representatives and the Secretary of State, who shall be trustees ex-officiis. Four other persons are appointed by the governor, of whom one shall be appointed annually for a four-year term commencing June first of the year of appointment. The board's chairman, who is elected by the board members, serves for a term of one year and the librarian serves as clerk to the board. To conduct official business, the board requires a quorum of four board members or their designees. The Library maintains its office at the State House, Room 341, in Boston. The Library supports a comprehensive web presence at www.state.ma.us/lib/.

Since its formal establishment, the Library's primary mission has been to maintain a position of vital importance to state government within the State House. Starting from a collection of maps, statute books, and government documents, the Library has grown into a multifaceted resource for legislators, executive personnel, state employees, historians, genealogists, and interested citizens.

The Library addresses its mission of meeting the research resource requirements of the branches of government and other users and as the official depository for Massachusetts state documents by providing:

- Professional and para-professional personnel to provide quality services;
- Full development of a strong and comprehensive collection of information materials in law, public affairs, current issues, and Massachusetts history;
- Automated library functions to provide better library services;
- Well-planned use of space for effective library services in a convenient location; and
- Preservation and conservation of library collections.

The Library uses information technology extensively to carry out its mission. At the time of our audit, the Library's information technology operations were supported by two file servers, 55 desktop computers, one laptop and one CD tower. The Library operates and supports two separate networks. The local area network (LAN) resides behind the Commonwealth's firewall and connects staff workstations to the file servers, CD Tower, and the Commonwealth's WAN. In June of 2001, the Library migrated to the Windows 2000 environment and staff desktop workstations were upgraded to Windows 2000 and Office 2000. The Library migrated from a Windows NT 4.0 sever to new server running Windows 2000. The workstations use the

Windows NT 4.0 operating system. Security software was being used to help prevent unauthorized access to the workstations. The Library also completed the migration to the Commonwealth's new email system, known as MassMail. Administration and Finance's Central Business Office provides the Library with standard business functions that includes Human Resources / Compensation Management System (HR/CMS) and Massachusetts Management Accounting and Reporting System (MMARS). The Library does not develop or maintain in-house applications, but instead uses standard business software and library automation software to perform daily work activities.

The Library provides electronic access to book collections via the Central / Western Massachusetts Automated Resource Sharing (C/WMARS) network, a library automation network located in Paxton. The C/WMARS network, which is external to the Commonwealth's firewall, provides the public with electronic access to library collections and the Internet.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From November 29, 2001 to December 17, 2001, we performed an information technology (IT) audit at the George E. Fingold Library covering the period of July 1, 2000 through December 17, 2001. Our audit scope included an examination of internal controls over selected information technology functions. We evaluated IT-related controls pertaining to physical security, environmental protection, logical access security, inventory control, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media.

Audit Objectives

The primary objective of our audit was to determine whether adequate controls were in place and in effect to provide a properly controlled IT environment. We sought to determine whether adequate controls regarding physical security and environmental protection were in place and in effect to safeguard computer operations and IT-related assets. With respect to system access security, we sought to determine whether adequate controls were in place to prevent and detect unauthorized access to system and application software and related data files residing on the Library's LAN-based file servers and desktop computers. Our objective with respect to hardware inventory was to determine whether IT-related assets were properly identified, recorded, and accounted for in the Library's inventory system of record.

With respect to the availability of automated processing capabilities and access to electronic information resources, we determined whether disaster recovery and business continuity controls would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether proper backup procedures were being performed and whether copies of backup magnetic media were stored in secure on-site and off-site locations.

Audit Methodology

To determine the scope of the audit, we performed a pre-audit survey regarding the Library's overall mission and its IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures and other internal control documentation; and observation of IT-related areas. To obtain an understanding of the Library's activities and internal control environment, we reviewed its mission, organizational structure, and primary

business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over the LAN file servers and desktop computers through observation, interviews with Library management and staff, documentation review, and completion of appropriate audit checklists. We reviewed the extent to which IT related resources were properly accounted for to determine whether the inventory would assist the Library in identifying IT resources under their charge.

We reviewed Library's logical access security policies and procedures to prevent and detect unauthorized access to software and data files residing on the Library's LAN. We discussed the security policies and procedures with the Systems Director who is responsible for controlling the Library's access to Information Technology Division (ITD)'s mainframe to which the Library is connected and the Library's LAN and desktop computers. Our examination of logical access security did not include a review of the Library staff's access privileges to the Commonwealth's Information Technology Division's (ITD) mainframe located at the ITD data center. We reviewed access privileges of the Library's staff who had been authorized to access applications residing on the LAN and the desktop computers. Subsequently, we determined whether all system users authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of password changes. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed procedures for authorizing access to the Library's IT resources on the LAN and desktop computers. We then determined whether individuals granted access to the Library's systems were currently employed by the Library by comparing an automated list of individuals authorized to access the automated systems to the Library's official employee list as contained in current payroll records.

To determine whether IT resources were properly accounted for, we reviewed inventory policies and procedures, interviewed appropriate staff, and examined the Library's system of record for maintaining an inventory of equipment. To determine whether the Library's hardware inventory record was accurate, complete, current, and valid, we reviewed inventory data for 57 items (100%) of computer equipment located at the Library. Moreover, to determine whether all hardware that was physically located at the Library was listed on the inventory record, we traced 57 items (100%) to the inventory records. Further, to test whether purchased hardware was being listed on the system of record for inventory and physically located at the Library, we

compared purchase orders and invoices for seven selected items of hardware purchased by the Library during fiscal year 2001 to the inventory records and located the individual hardware items at the Library offices. We also determined whether computer equipment was properly tagged and verified the tag numbers to the inventory record. We compared the state identification or tag numbers listed on the inventory record to the actual item of equipment on hand.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the level of planning and established procedures to be followed to resume computer operations in the event that the file servers and desktop computers were rendered inoperable or inaccessible. We interviewed Library management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been identified and evaluated, whether a written business continuity plan was in place, and, if so, whether it had been adequately tested. The interview also addressed an evaluation of the adequacy of controls to ensure that software and data files would be available for recovery efforts should the automated systems be rendered inoperable. The latter included a review of the adequacy of provisions for on-site and off-site storage of critical backup tapes. In that regard, we interviewed the Library staff responsible for creating and storing backup copies of IT-related media.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted auditing practices. Audit criteria used in the audit included management policies and procedures, and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT) as issued by the Information Systems Audit and Control Association, July 2000. CobiT control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices that provides a reference framework for management, users, security practitioners, and auditors.

AUDIT SUMMARY

Based on our audit, we found that information technology-related controls in place at the George E. Fingold Library provided reasonable assurance that the Library's computer environment was sufficiently controlled to support its automated systems, except for the requirement to strengthen business continuity planning and off-site storage of backup copies of magnetic media.

Our audit revealed that adequate physical security and environmental protection were being provided for the Library's IT-related assets. In this regard, we found that areas housing computer equipment were appropriately secured and alarmed, fire detection and suppression controls were in place, processing areas were well maintained, a fire emergency plan was in place and posted, and appropriate air quality was afforded to the file server room.

Adequate controls were found to be in place to provide reasonable assurance that only authorized users would be permitted access to the Library's automated systems. In addition, by the end of the audit, the Library had all staff who were system users sign a computer usage form. The Library had fully implemented this control to help ensure that users were aware of and understood their responsibilities regarding acceptable use, data confidentiality, copyright protection, virus protection, security, and e-mail usage.

We found that the Library had appropriate controls in place to provide reasonable assurance that IT resources would be properly accounted for on the Library's system of record for its equipment inventory. Our audit tests indicated that the inventory system of record was accurate, complete, current, and valid for IT resources. We also found that computer equipment was properly tagged and that equipment purchased within the past year was properly recorded on the inventory and could be readily located at the Library. Given that adequate physical security and inventory control policies and practices were found to be in place, there was reasonable assurance that computer equipment would be properly accounted for and safeguarded.

With regard to the continued availability of computer operations and access to electronic information, we found that disaster recovery and business continuity plans needed to be strengthened. Although the Library generated and stored backup copies of magnetic media at on-site and off-site locations, the off-site location did not afford sufficient assurance that appropriate controls would be in effect for the security and ongoing availability of backup media. With respect to recovery strategies and contingency plans, we found that although the Library had a formal, tested business continuity plan dealing with circumstances that could physically threaten the Library's collections, the plan did not address information technology requirements,

or those automated systems that would need to be recovered in the event that IT resources were rendered inoperable or inaccessible. Without sufficient business continuity planning for IT resources, including a viable alternate-processing site, a possible long-term loss of the Library's computer operations could hinder access to processing capabilities and electronic information needed to perform business functions.

We recommend that the Library assess the relative criticality of its automated systems and conduct a formal risk analysis of its IT components, including outsourced services. Based on the results of the criticality assessment and risk analysis, the Library should confirm its understanding of business continuity requirements and, as necessary, amend recovery plans to address mission-critical and essential IT-supported business functions and services.

AUDIT RESULTS

1. Disaster Recovery and Business Continuity Planning

The George E. Fingold Library's business continuity plan, which addresses book, map, and document collections, needed to be expanded to address information technology requirements to provide reasonable assurance that mission-critical IT operations could be regained effectively and in a timely manner should computer systems be rendered inoperable or inaccessible. Although backup copies of mission-critical and essential software and data files were being generated, specific arrangements had not been made to provide for alternate-site processing. In this regard, we found that there was no agreement in place with another organization for alternate-site processing should the Library's IT systems be unusable or inaccessible. Although the Library had not formally assessed the relative criticality of its automated systems, management was aware of the relative importance of their application systems to the mission of the Library. We found, however, that a detailed risk analysis had not been performed to identify and determine the extent of potential risks and exposures to the Library's data processing operations. Information obtained from a detailed risk analysis not only assists an entity in addressing business continuity planning but also helps ensure that appropriate internal control measures are implemented. Our audit revealed that the Library's functional business process areas had not developed user-area contingency plans to address a potential loss of their automated processing.

Regarding the generation and storage of backup copies of mission-critical and essential software and data files, we found that backup copies were generated on a daily basis and that on-site storage of backup tapes was being carried out effectively. Although backup tapes were being stored off-site, we found the use of an employee's home to provide off-site backup media storage was unacceptable because this arrangement would not permit a reasonable level of assurance regarding required security, environmental protection, access-on-demand as necessary, and independent review and testing.

Without adequate disaster recovery and business continuity planning, including required user-area plans, the Library was at risk of severely degraded or failed processing should automated capabilities be disrupted or lost. Based upon our audit, it appeared that the Library's operations would be adversely impacted should automated processing not be regained within a week's time period. We found that a loss of processing capabilities could adversely affect all functions supported by the file servers. Furthermore, the absence of a comprehensive and tested disaster

recovery and business continuity plan could result in unnecessary costs, significant processing delays and loss of goodwill.

Disaster recovery and business continuity plans should be in place to direct recovery procedures, first, for the most important IT-based operations and, second, for less essential operations. A formal criticality assessment assists management in establishing recovery and contingency plans using a triaged approach whereby resources and plans are allocated to mission-critical operations first, and then to lesser important IT operations.

Disaster recovery and business continuity plans should be well tested to reduce time and the risk of errors and omissions when restoring computer operations. An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the file servers and, accordingly, the manner in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, advocate that a comprehensive and effective backup and disaster recovery and business continuity plan be in place. Contingency planning should be viewed as a process to be incorporated with the functions of the organization, rather than as a project with successful completion upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that would identify a change in criticality and amend the contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans. Business continuity and contingency planning has taken on added importance given potential processing disruptions that could be caused by man-made events.

Recommendation:

The Library should formally assess the relative criticality of automated systems to identify application priorities and critical resources. A risk analysis should be conducted to identify risks and exposures relating to the Library's data processing operations and IT environment. The Library should identify potential processing alternatives and resources to be used should a

disaster disrupt data processing or business operations. Based upon these results, and input solicited from management and user departments, a written disaster recovery and business continuity plan should be developed, reviewed, tested to the extent possible, approved by senior management, and implemented.

We further recommend that procedures be developed to ensure that the relative criticality of automated systems is periodically reassessed, that the impact of changes in user needs or automated systems be evaluated, and that staff are adequately trained in executing recovery and contingency plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is appropriate, current, accurate, and complete. The plan, or specific sections of it, should be distributed to appropriate personnel, and a complete copy of the plan should be stored in a secure off-site location.

We also recommend that the Library relocate off-site storage of backup media from an employee's home to a site under the charge of the Library, or another state agency where the provision of adequate internal controls can be assured with a higher level of confidence and be subject to independent examination.

Auditee's Response:

1. The Library already has a disaster plan, which, however, is in need of updating anyway. It does not contain an IT section.

Therefore, the Library will update its disaster recovery plan (including a new developed business continuity plan), which will be reviewed and tested to the extent possible and approved by senior management and the Board of Trustees.

It will be based upon input from senior management and user departments and upon the results of a number of studies made by Library staff. The Library will formally assess the relative criticality of automated systems to identify application priorities and critical resources. The Library will conduct a risk analysis to identify risks and exposures relating to the Library's data processing operations and IT environment. The Library will identify potential processing alternatives and resources to be used should a disaster disrupt data processing or business operations.

2. The Library commits itself to develop procedures to ensure that it periodically reassesses the relative criticality of automated systems and to evaluate the impact of charges in user needs or automated systems. Upon a major change to systems or equipment or, at least, annually, the Library will review, update, and test its disaster recovery plan to ensure that it is appropriate, current, accurate, and complete. The Library will distribute to appropriate personnel the plan or specific sections of it and will store in a secure off-site location a complete copy of the plan.

3. The Library will relocate off-site storage of backup media from an employee's home to another state agency where the provision of adequate

internal controls can be assured with a higher level of confidence and be subject to independent examination.

Auditor's Reply:

We are pleased that the Library intends to develop an IT section within its business continuity plan and concur with the steps to be taken above. Once the key elements of the business continuity plan are developed, they should be documented, tested, reviewed, and approved. We suggest that appropriate training be provided to ensure that business continuity plan procedures are sufficiently understood. We agree with the approach of developing processing alternatives. Given that IT processing requirements, or that of the relationship with the agency providing alternative processing capabilities might change over time, we suggest that the requirements and responsibilities of both parties be documented and periodically re-evaluated to permit timely changes. Understandably, until the recovery and continuity plan is fully developed, the Library would remain vulnerable from a business continuity perspective.